

日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

09/504070

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 9月 1日

出願番号

Application Number:

平成11年特許願第247457号

出願人

Applicant(s):

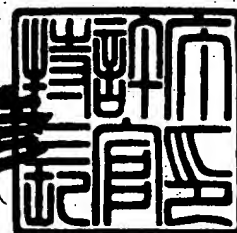
日本電信電話株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 1月14日

特許庁長官  
Commissioner,  
Patent Office

近藤隆彦



【書類名】 特許願

【整理番号】 NTTH115883

【提出日】 平成11年 9月 1日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 G06F 15/21

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 寺田 雅之

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 藤村 考

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 久野 浩

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 花館 蔵之

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100070150

【弁理士】

【氏名又は名称】 伊東 忠彦

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項 1】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報と、から構成される原本性情報を転送する転送手段を有する第 1 の装置と、

前記原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第 1 の認証手段と、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第 2 の認証手段とを有する第 2 の装置とを有することを特徴とする原本データ流通システム。

【請求項 2】 前記第 1 の装置は、

秘密鍵を秘匿する手段を更に有し、

前記第 2 の装置は、

1 乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手する手段を更に有し、

前記第 2 の装置の前記第 1 の認証手段は、

転送元の前記第 1 の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第 1 の装置を認証する請求項 1 記載の原本データ流通システム。

【請求項 3】 前記第 1 の装置の前記転送手段は、

自装置が 1 乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を前記第 2 の装置に転送する手段を有し、

前記第 2 の装置は、

1 乃至複数の第三者に対応する第三者情報を保持、または、入手する手段を有

し、

前記第 1 の認証手段は、

転送元装置である前記第 1 の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第 1 の装置を認証する請求項 1 記載の原本データ流通システム。

【請求項 4】 前記第 2 の装置は、

前記第 1 の情報と、 1 乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手する手段を有し、

前記第 1 の認証手段は、

原本性情報の転送元である前記第 1 の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第 1 の情報から、保持されている前記第三者信任情報を用いて該第 1 の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証する請求項 3 記載の原本データ流通システム。

【請求項 5】 前記第 2 の装置は、

前記第 1 の情報と前記第 2 の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手する手段を有し、

前記第 1 の認証手段は、

転送された前記原本性情報の前記第 1 の情報と前記第 2 の情報から、前記第三者信任情報を用いて該第 1 の情報と該第 2 の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証する請求項 3 記載の原本データ流通システム。

【請求項 6】 前記第 1 の装置は、

秘密鍵を秘匿する手段と、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第 2 の装置に転送する手段を有し、

前記第 2 の装置は、

前記公開鍵証明書を検証して署名者の公開鍵を特定する手段と、

1 乃至複数のフィガープリントを保持または、入手する手段とを更に有し、

前記第 1 の認証手段は、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、  
該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前  
記フィンガープリントに含まれることを検証することにより、転送元の前記第 1  
の装置を認証する請求項 1 記載の原本データ流通システム。

【請求項 7】 前記第 2 の装置は、

前記第 1 の情報と、 1 乃至複数の第 1 の装置に対応する情報とを対応付ける利  
用者信任情報を保持もしくは、入手する手段を有し、

前記第 1 の認証手段は、

転送された前記原本性情報の第 1 の情報から、保持されている前記利用者信任  
情報を用いて、該第 1 の情報に対応する第 1 の装置に対応する情報を抽出し、転  
送元装置が該利用者信任情報から抽出された第 1 の装置に含まれることを検証す  
ることにより、該転送元の第 1 の装置を認証する請求項 1 記載の原本データ流通  
システム。

【請求項 8】 前記第 2 の装置は、

前記第 1 の情報と前記第 2 の情報から、 1 乃至複数の前記第 1 の装置に対応す  
る情報を対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

前記第 1 の認証手段は、

転送された前記原本性情報の第 1 の情報と第 2 の情報とから、保持されている  
前記利用者信任情報を用いて、該第 1 の情報と該第 2 の情報に対応する第 1 の装  
置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第  
1 の装置に含まれることを検証することにより、該転送元の第 1 の装置を認証す  
る請求項 1 記載の原本データ流通システム。

【請求項 9】 電子的な情報である原本データの蓄積や流通を行う原本デー  
タ流通システムであって、

自装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対

応する情報を第2の情報として、原本性情報を生成する原本性情報生成手段と、  
前記原本性情報を転送する原本性情報転送手段とを有する発行者装置を有することを特徴とする原本データ流通システム。

【請求項10】 前記発行者装置は、  
秘密鍵を秘匿する手段と、  
前記秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを前記第1の情報として生成する手段を有する請求項9記載の原本データ流通システム。

【請求項11】 前記発行者装置は、  
前記原本性情報の前記第2の情報として、データの一方向関数による出力を生成する手段を有する請求項9記載の原本データ流通システム。

【請求項12】 前記発行者装置は、  
前記原本性情報の前記第2の情報として、ネットワーク上の資源の識別子を用いる請求項11記載の原本データ流通システム。

【請求項13】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報から構成される原本性情報を転送する原本性情報転送手段と、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、

前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、

前記認証手段で前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置を有することを特徴とする原本データ流通システム。

【請求項14】 前記利用者装置は、  
自装置から前記原本性情報を転送する際に、該原本性情報を消去する手段を有する請求項13記載の原本データ流通システム。

【請求項 15】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

原本性情報の転送元装置を特定する特定手段と、

前記転送元装置を認証する認証手段と、

前記認証手段において、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対応する処理を行うデータ処理手段を有する改札者装置を有することを特徴とする原本データ流通システム。

【請求項 16】 前記改札者装置は、

発行者装置に対応する情報である発行者情報を保持もしくは、入手する手段を更に有し、

前記データ処理手段は、

前記認証手段において、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第1の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第2の情報に対応するデータに対する処理を行う請求項 15 記載の原本データ流通システム。

【請求項 17】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第1の情報とし、あるデータもしくは、該データに対応する情報を第2の情報として、原本性情報を生成する第1の原本性情報生成手段と、該原本性情報を転送する第1の原本性情報転送手段とを有する発行者装置と、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報から構成される原本性情報を転送する第2の原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第1の特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第1の認証手段と、該第1の認証手段で該原



本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置と、

原本性情報の転送元装置を特定する第 2 の特定手段と、前記転送元装置を認証する第 2 の認証手段と、該第 2 の認証手段において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第 2 の情報に対応するデータに対する処理を行うデータ処理手段を有する改札者装置とを有することを特徴とする原本データ流通システム。

【請求項 1 8】 電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

第 1 の装置に搭載される、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報と、から構成される原本性情報を転送させる転送プロセスと、

第 2 の装置に搭載される、

前記原本性情報の転送元装置を特定する特定プロセスと、該転送元装置が認証された場合に該原本性情報を有効であると判別する第 1 の認証プロセスと、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第 2 の認証プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項 1 9】 前記第 1 の装置に搭載される、秘密鍵を秘匿するプロセスを更に有し、

前記第 2 の装置に搭載される、

1 乃至、複数の秘密鍵に対応する公開鍵の一方向性関数による出力である自装置のフィンガープリントを保持、または、入手するプロセスを更に有し、

前記第 1 の認証プロセスは、

転送元の前記第 1 の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む請求項 1 8 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 0】 前記第 1 の装置に搭載されるの前記転送プロセスは、自装置が 1 乃至複数の第三者によって認証されていることを証明する情報であ

り、該第三者である認証者に対応する情報である第三者証明を前記第2の装置に転送するプロセスを有し、

前記第2の装置に搭載される、

1乃至複数の第三者に対応する第三者情報を保持、または、入手するプロセスを有し、

前記第2の装置に搭載される前記第1の認証プロセスは、

転送元装置である前記第1の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第1の装置を認証するプロセスを含む請求項18記載の原本データ流通プログラムを格納した記憶媒体。

【請求項21】 前記第2の装置に搭載される、

前記第1の情報と、1乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するプロセスを有し、

前記第1の認証プロセスは、

原本性情報の転送元である前記第1の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第1の情報から、保持されている前記第三者信任情報を用いて該第1の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第1の装置を認証するプロセスを含む請求項20記載の原本データ流通プログラムを格納した記憶媒体。

【請求項22】 前記第2の装置に搭載される、

前記第1の情報と前記第2の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手するプロセスを有し、

前記第1の認証プロセスは、

転送された前記原本性情報の前記第1の情報と前記第2の情報から、前記第三者信任情報を用いて該第1の情報と該第2の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第1の装置を認証

するプロセスを含む請求項 2 0 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 3】 前記第 1 の装置に搭載される、

秘密鍵を秘匿するプロセスと、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第 2 の装置に転送するプロセスを有し、

前記第 2 の装置に搭載される、

前記公開鍵証明書を検証して署名者の公開鍵を特定するプロセスと、

1 乃至複数のフィガープリントを保持または、入手するプロセスとを更に有し

、  
前記第 1 の認証プロセスは、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第 1 の装置を認証するプロセスを含む請求項 1 8 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 4】 前記第 2 の装置に搭載される、

前記第 1 の情報と、1 乃至複数の第 1 の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第 1 の認証プロセスは、

転送された前記原本性情報の第 1 の情報から、保持されている前記利用者信任情報を用いて、該第 1 の情報に対応する第 1 の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第 1 の装置に含まれることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む請求項 1 8 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 5】 前記第 2 の装置に搭載される、

前記第 1 の情報と前記第 2 の情報から、1 乃至複数の前記第 1 の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第 1 の認証プロセスは、

転送された前記原本性情報の第 1 の情報と第 2 の情報とから、保持されている前記利用者信任情報を用いて、該第 1 の情報と該第 2 の情報に対応する第 1 の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第 1 の装置に含まれることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む請求項 1 8 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 6】 電子的な情報である原本データの蓄積や流通を行う発行者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

前記発行者装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対応する情報を第 2 の情報として、原本性情報を生成する原本性情報生成プロセスと、

前記原本性情報を転送する原本性情報転送プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項 2 7】 秘密鍵を秘匿するプロセスと、

前記秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを前記第 1 の情報として生成するプロセスを有する請求項 2 6 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 8】 前記原本性情報の前記第 2 の情報として、データの一方向関数による出力を生成するプロセスを有する請求項 2 6 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 2 9】 前記原本性情報の前記第 2 の情報として、ネットワーク上の資源の識別子を用いるプロセスを含む請求項 2 8 記載の原本データ流通プログラムを格納した記憶媒体。

【請求項 3 0】 電子的な情報である原本データの蓄積や流通を行う利用者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報から構成される原本性情報を転送する原本性情報転送プロセスと

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定

する特定プロセスと、

前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証プロセスと、

前記認証プロセスで前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項31】 前記利用者装置から前記原本性情報を転送する際に、該原本性情報を消去するプロセスを有する請求項30記載の原本データ流通プログラムを格納した記憶媒体。

【請求項32】 電子的な情報である原本データの蓄積や流通を行う改札者装置に搭載される原本データ流通プログラムであって、

原本性情報の転送元装置を特定する特定プロセスと、

前記転送元装置を認証する認証プロセスと、

前記認証プロセスにおいて、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対応する処理を行うデータ処理プロセスを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項33】 発行者装置に対応する情報である発行者情報を保持もしくは、入手するプロセスを更に有し、

前記データ処理プロセスは、

前記認証プロセスにおいて、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第1の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第2の情報に対応するデータに対する処理を行う請求項32記載の原本データ流通プログラムを格納した記憶媒体。

【請求項34】 電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に搭載される、

前記発行者装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対応する情報を第 2 の情報として、原本性情報を生成する第 1 の原本性情報生成プロセスと、

前記原本性情報を転送する第 1 の原本性情報転送プロセスと、

利用者装置に搭載される、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報から構成される原本性情報を転送する第 2 の原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第 1 の特定プロセスと、

前記転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第 1 の認証プロセスと、

前記第 1 の認証プロセスで該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスと、

改札者装置に搭載される、

原本性情報の転送元装置を特定する第 2 の特定プロセスと、

前記転送元装置を認証する第 2 の認証プロセスと、

前記第 2 の認証プロセスにおいて、前記改札者装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第 2 の情報に対応するデータに対する処理を行うデータ処理プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体に係り、特に、電子チケットなどの権利を表象するデータやデジタル著作物など、有効な複製数を一定数以下に保つことが必要とされるデータについ

て、蓄積や配送のための手段を提供するための原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体に関する。

【0002】

【従来の技術】

権利を表象したデータや著作物などは、配布者などの意図する数を越えて同時に複製が存在することを防止することが求められる。即ち、配布したデータが利用者などにより複製され、それらが多重に利用されることを防ぐ必要がある。

従来は、以下で示すような技術によりそのような多重利用を防止している。

【0003】

第1の方法として、権利を表象するデータについて、権利の提供者などにより該データの使用履歴を保持しておき、権利の行使時に、当該データが既に使用されていないかどうかを検証する。もし、既に使用されていれば、当該データが表象する権利の行使を拒否する。

第2の方法として、データ自身を耐タンパ装置に格納し、当該データを当該耐タンパ装置の外からは参照できないようにする。権利の行使時には、当該データを該耐タンパ装置より抹消する。

【0004】

第3の方法として、データ自身は通常の蓄積媒体に格納するが、当該データの原本性を示すデータ（トークン）のみを耐タンパ装置に格納する。権利の行使時には、そのトークンを当該耐タンパ装置より抹消する。

【0005】

【発明が解決しようとする課題】

しかしながら、上記従来の第1の方法では、耐タンパ装置など特別な装置を必要としないが、該データを転々と流通させる際には、問題が生じる。すなわ、当該技術では、行使時の事後検出しか行えないため、流通過程では、当該データの有効性は判定できないという問題がある。

【0006】

従来の第2の方法では、耐タンパ装置を用いることにより、データの唯一性を保証することができる。また、「特表平6-503913」や「特表平9-51

1350」などで述べられている方式などを併用し、暗号によって保護された安全な通信路を介して耐タンパ装置を結合し、当該通信路を介してデータの授受を行うことにより、該データの流通を、複製を事前防止しながら行うことが可能とする。しかしながら、当該技術は、耐タンパ装置の中にデータを格納する必要があるため、以下の2点が問題となる。

【0007】

まず、データの記述そのものを見ることができなくなるため、記述の正当性の検証など、複製に関する有効性以外の検証も全て該タンパ装置に委ねなければならないという制約が生ずる。

また、データの格納部のみならず、データの取扱に必要な処理も全て耐タンパ装置が負わなければならないため、耐タンパ装置に対して記憶容量や処理速度に大きな要求が発生する。特に、現時点で耐タンパ装置として一般的なICカードでは、処理速度や記憶容量に不足が生じる。

【0008】

従来の第3の方法は、原本性を示すデータであるトークンのみを耐タンパ装置に格納することにより、データの有効な複製数を常に一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証を全て耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させる（特願平11-39080）。しかしながら、該技術では、実用上主に、以下の2点が問題となる。

【0009】

まず、トークンの生成時に、データと該データに付与された署名を検証するためにデータ及び該データの署名を耐タンパ装置に転送しなくてはならず、その一方で、ICカードの転送速度は、9600bit/s程度（ISO-7816）と比較的低速であるため、耐タンパ装置としてICカードを用いると、該データの大きさによってはトークンの生成に要する時間を著しく増大させる。

【0010】

また、当該技術では、データに対して署名を付与したものに対してトークンを生成し、消費の際にも該データ及び該署名を用いてトークンの検証が必要となる



ため、該データのみならず、該署名も共に流通させる必要が生じ、これは、システムに構築のために必要な記憶容量や流通の際の処理時間を増大させる。

本発明は、上記の点に鑑みなされたもので、従来の第 3 の方法におけるトークンの生成やデータの流通などにおける負荷を低減する原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】

本発明（請求項 1）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報と、から構成される原本性情報を転送する転送手段を有する第 1 の装置と、

原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第 1 の認証手段と、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第 2 の認証手段とを有する第 2 の装置とを有する。

【0012】

本発明（請求項 2）は、第 1 の装置において、

秘密鍵を秘匿する手段を更に有し、

第 2 の装置において、

1 乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手する手段を更に有し、

第 2 の装置の第 1 の認証手段において、

転送元の第 1 の装置がフィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第 1 の装置を認証する。

【0013】

本発明（請求項 3）は、第 1 の装置の転送手段において、

当該第 1 の装置が 1 乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を第 2 の装

置に転送する手段を有し、

第 2 の装置において、

1 乃至複数の第三者に対応する第三者情報を保持、または、入手する手段を有し、

当該第 2 の装置の第 1 の認証手段において、

転送元装置である第 1 の装置が第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている第三者情報に対応する第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証する。

【0 0 1 4】

本発明（請求項 4）は、第 2 の装置において、

第 1 の情報と、1 乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手する手段を有し、

当該第 2 の装置の第 1 の認証手段において、

原本性情報の転送元である第 1 の装置が該第三者証明における認証対象であり、かつ、転送された原本性情報の第 1 の情報から、保持されている第三者信任情報を用いて該第 1 の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証する。

【0 0 1 5】

本発明（請求項 5）は、第 2 の装置において、

第 1 の情報と第 2 の情報とから、第三者に対応する情報とを対応づける、第三者信任情報を保持もしくは、入手する手段を有し、

当該第 2 の装置の第 1 の認証手段において、

転送された原本性情報の第 1 の情報と第 2 の情報から、第三者信任情報を用いて該第 1 の情報と該第 2 の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証する。

【0 0 1 6】

本発明（請求項 6）は、第 1 の装置において、

秘密鍵を秘匿する手段と、

秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を第 2 の装置に転送する手段を有し、

第 2 の装置において、

公開鍵証明書を検証して署名者の公開鍵を特定する手段と、

1 乃至複数のフィガープリントを保持または、入手する手段とを更に有し、

当該第 2 の装置の第 1 の認証手段において、

秘密鍵による署名を公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されているフィンガープリントに含まれることを検証することにより、転送元の第 1 の装置を認証する。

【0017】

本発明（請求項 7）は、第 2 の装置において、

第 1 の情報と、1 乃至複数の第 1 の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

第 1 の認証手段において、

転送された原本性情報の第 1 の情報から、保持されている利用者信任情報を用いて、該第 1 の情報に対応する第 1 の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第 1 の装置に含まれることを検証することにより、該転送元の第 1 の装置を認証する。

【0018】

本発明（請求項 8）は、第 2 の装置において、

第 1 の情報と第 2 の情報から、1 乃至複数の第 1 の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

第 1 の認証手段において、

転送された原本性情報の第 1 の情報と第 2 の情報とから、保持されている利用者信任情報を用いて、該第 1 の情報と該第 2 の情報に対応する第 1 の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第 1 の装置に含まれることを検証することにより、該転送元の第 1 の装置を認証する。

【0 0 1 9】

本発明（請求項 9）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対応する情報を第 2 の情報として、原本性情報を生成する原本性情報生成手段と、  
原本性情報を転送する原本性情報転送手段とを有する発行者装置を有する。

【0 0 2 0】

本発明（請求項 1 0）は、発行者装置において、  
秘密鍵を秘匿する手段と、

秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを第 1 の情報として生成する手段を有する。

本発明（請求項 1 1）は、発行者装置において、

原本性情報の第 2 の情報として、データの一方向関数による出力を生成する手段を有する。

【0 0 2 1】

本発明（請求項 1 2）は、発行者装置において、

原本性情報の第 2 の情報として、ネットワーク上の資源の識別子を用いる。

本発明（請求項 1 3）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報から構成される原本性情報を転送する原本性情報転送手段と、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、

転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、

認証手段で原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置を有する。

【0 0 2 2】

本発明（請求項 1 4）は、利用者装置において、

自装置から原本性情報を転送する際に、該原本性情報を消去する手段を有する

本発明（請求項 1 5）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

原本性情報の転送元装置を特定する特定手段と、

転送元装置を認証する認証手段と、

認証手段において、自装置に転送された原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第 2 の情報に対応するデータに対応する処理を行うデータ処理手段を有する改札者装置を有する。

【 0 0 2 3 】

本発明（請求項 1 6）は、改札者装置において、

発行者装置に対応する情報である発行者情報を保持もしくは、入手する手段を更に有し、

データ処理手段において、

認証手段において転送された原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第 1 の情報に対応する発行者装置が、保持されている発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第 2 の情報に対応するデータに対する処理を行う。

【 0 0 2 4 】

図 1 は、本発明の原理構成図である。

本発明（請求項 1 7）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対応する情報を第 2 の情報として、原本性情報を生成する第 1 の原本性情報生成手段 1 1 0 と、該原本性情報を転送する第 1 の原本性情報転送手段 1 2 0 とを有する発行者装置 1 0 0 と、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報で

ある第 2 の情報から構成される原本性情報を転送する第 2 の原本性情報転送手段 2 1 0 と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第 1 の特定手段 2 2 0 と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第 1 の認証手段 2 3 0 と、該第 1 の認証手段 2 3 0 で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段 2 4 0 とを有する利用者装置 2 0 0 と、

原本性情報の転送元装置を特定する第 2 の特定手段 3 1 0 と、転送元装置を認証する第 2 の認証手段 3 2 0 と、該第 2 の認証手段 3 2 0 において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第 2 の情報に対応するデータに対する処理を行うデータ処理手段 3 3 0 を有する改札者装置 3 0 0 とを有する。

【 0 0 2 5 】

本発明（請求項 1 8）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

第 1 の装置に搭載される、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報と、から構成される原本性情報を転送させる転送プロセスと、

第 2 の装置に搭載される、

原本性情報の転送元装置を特定する特定プロセスと、該転送元装置が認証された場合に該原本性情報を有効であると判別する第 1 の認証プロセスと、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第 2 の認証プロセスとを有する。

【 0 0 2 6 】

本発明（請求項 1 9）は、第 1 の装置に搭載される、秘密鍵を秘匿するプロセスを更に有し、

第 2 の装置に搭載される、

1 乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手するプロセスを更に有し、

第 1 の認証プロセスにおいて、

転送元の第 1 の装置がフィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む。

【 0 0 2 7 】

本発明（請求項 2 0）は、第 1 の装置に搭載されるの転送プロセスにおいて、

自装置が 1 乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を第 2 の装置に転送するプロセスを有し、

第 2 の装置に搭載される、

1 乃至複数の第三者に対応する第三者情報を保持、または、入手するプロセスを有し、

第 2 の装置に搭載される第 1 の認証プロセスにおいて、

転送元装置である第 1 の装置が第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている第三者情報に対応する第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む。

【 0 0 2 8 】

本発明（請求項 2 1）は、第 2 の装置に搭載される、

第 1 の情報と、 1 乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するプロセスを有し、

第 2 の装置に搭載される第 1 の認証プロセスにおいて、

原本性情報の転送元である第 1 の装置が該第三者証明における認証対象であり、かつ、転送された原本性情報の第 1 の情報から、保持されている第三者信任情報を用いて該第 1 の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む。

【 0 0 2 9 】

本発明（請求項 2 2）は、第 2 の装置に搭載される、

第 1 の情報と第 2 の情報とから、第三者に対応する情報とを対応づける、第三

者信任情報を保持もしくは、入手するプロセスを有し、

第 2 の装置に搭載される第 1 の認証プロセスにおいて、

転送された原本性情報の第 1 の情報と第 2 の情報から、第三者信任情報を用いて該第 1 の情報と該第 2 の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む。

【 0 0 3 0 】

本発明（請求項 2 3）は、第 1 の装置に搭載される、

秘密鍵を秘匿するプロセスと、

秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を第 2 の装置に転送するプロセスを有し、

第 2 の装置に搭載される、

公開鍵証明書を検証して署名者の公開鍵を特定するプロセスと、

1 乃至複数のフィガープリントを保持または、入手するプロセスとを更に有し

第 2 の装置に搭載される第 1 の認証プロセスにおいて、

秘密鍵による署名を公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されているフィンガープリントに含まれることを検証することにより、転送元の第 1 の装置を認証するプロセスを含む。

【 0 0 3 1 】

本発明（請求項 2 4）は、第 2 の装置に搭載される、

第 1 の情報と、1 乃至複数の第 1 の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

第 2 の装置に搭載される第 1 の認証プロセスにおいて、

転送された原本性情報の第 1 の情報から、保持されている利用者信任情報を用いて、該第 1 の情報に対応する第 1 の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第 1 の装置に含まれることを検証することに



より、該転送元の第 1 の装置を認証するプロセスを含む。

【0032】

本発明（請求項 25）は、第 2 の装置に搭載される、

第 1 の情報と第 2 の情報から、1 乃至複数の第 1 の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

第 2 の装置に搭載される第 1 の認証プロセスにおいて、

転送された原本性情報の第 1 の情報と第 2 の情報とから、保持されている利用者信任情報を用いて、該第 1 の情報と該第 2 の情報に対応する第 1 の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第 1 の装置に含まれることを検証することにより、該転送元の第 1 の装置を認証するプロセスを含む。

【0033】

本発明（請求項 26）は、電子的な情報である原本データの蓄積や流通を行う発行者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対応する情報を第 2 の情報として、原本性情報を生成する原本性情報生成プロセスと、

原本性情報を転送する原本性情報転送プロセスとを有する。

【0034】

本発明（請求項 27）は、秘密鍵を秘匿するプロセスと、

秘密鍵に対応する公開鍵の一方向関数による出力である発行者装置のフィンガープリントを第 1 の情報として生成するプロセスを有する。

本発明（請求項 28）は、原本性情報の第 2 の情報として、データの一方向関数による出力を生成するプロセスを有する。

【0035】

本発明（請求項 29）は、原本性情報の第 2 の情報として、ネットワーク上の資源の識別子を用いるプロセスを含む。

本発明（請求項 30）は、電子的な情報である原本データの蓄積や流通を行う

利用者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報から構成される原本性情報を転送する原本性情報転送プロセスと

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定プロセスと、

転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証プロセスと、

認証プロセスで原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスとを有する。

#### 【 0 0 3 6 】

本発明（請求項 3 1）は、利用者装置から原本性情報を転送する際に、該原本性情報を消去するプロセスを有する。

本発明（請求項 3 2）は、電子的な情報である原本データの蓄積や流通を行う改札者装置に搭載される原本データ流通プログラムであって、

原本性情報の転送元装置を特定する特定プロセスと、

転送元装置を認証する認証プロセスと、

認証プロセスにおいて、自装置に転送された原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第 2 の情報に対応するデータに対応する処理を行うデータ処理プロセスを有する。

#### 【 0 0 3 7 】

本発明（請求項 3 3）は、発行者装置に対応する情報である発行者情報を保持もしくは、入手するプロセスを更に有し、

データ処理プロセスにおいて、

認証プロセスにおいて、転送された原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第 1 の情報に対応する発行者装置が、保持されている発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデー

タまたは、データに対応する情報である第 2 の情報に対応するデータに対する処理を行う。

【 0 0 3 8 】

本発明（請求項 3 4）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に搭載される、

発行者装置に対応する情報を第 1 の情報とし、あるデータもしくは、該データに対応する情報を第 2 の情報として、原本性情報を生成する第 1 の原本性情報生成プロセスと、

原本性情報を転送する第 1 の原本性情報転送プロセスと、

利用者装置に搭載される、

ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報から構成される原本性情報を転送する第 2 の原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第 1 の特定プロセスと、

転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第 1 の認証プロセスと、

第 1 の認証プロセスで該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスと、

改札者装置に搭載される、

原本性情報の転送元装置を特定する第 2 の特定プロセスと、

転送元装置を認証する第 2 の認証プロセスと、

第 2 の認証プロセスにおいて、改札者装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第 2 の情報に対応するデータに対する処理を行うデータ処理プロセスとを有する。

【 0 0 3 9 】

上記の請求項 1 及び請求項 1 8 では、第 1 の装置は、装置を示す第 1 の情報と

データを示す第2の情報から構成される原本性情報を転送する手段を備え、第2の装置は、原本性情報の転送を受ける際に、第1の情報が示す装置が転送元装置であるか、もしくは、転送元装置が転送先装置にとって「信用できる」装置である場合のみ、原本性情報を有効であると判別することが可能となる。

【0040】

請求項2及び請求項19では、公開暗号系を用いて転送元装置を特定し、第2の装置が「信用する」利用者装置を示すフィンガープリントを用いて、転送元装置が信用できるかどうかを判断することが可能となる。

請求項3及び請求項20では、第1の装置が、当該装置が第三者である認証者に「信用されている」ことを証明する情報である第三者情報を第2の装置に転送する手段を備え、第2の装置は、当該装置が「信用する」第三者を示す情報である第三者情報を保持する手段と、第1の装置から原本性情報が転送された際に、当該原本性情報の転送元装置が第1の装置であり、かつ、第2の装置が保持する第三者情報が示す第三者に、当該第三者証明の認証者が含まれることを検証することにより、信用できるかどうかを判断することが可能となる。

【0041】

請求項4及び請求項21では、発行者層が「信用する」第三者装置を示す第三者信任情報と、第1の装置が第三者である認証者により認証されていることを示す第三者証明を用い、転送元の第1の装置が第三者証明の認証者により認証された装置であり、かつ、該認証者が原本性情報の第1の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用できる第1の装置を特定する情報を直接に指示することなく、信用できる第1の装置を発行者装置が指定することが可能となる。

【0042】

請求項5及び請求項22では、発行者装置が「信用する」第三者装置を示す第三者信任情報と、第1の装置が第三者である認証者により認証されていることを示す第三者証明を用い、転送元の第1の装置が当該第三者証明の認証者により認証された装置であり、かつ、当該認証者が原本性情報の第1の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用で

きる第1の装置を特定する情報を直接に指定することなく、信用できる第1の装置を発行者装置がデータ毎、もしくは、データの集合毎に指定することが可能となる。

## 【0043】

請求項6及び請求項23では、公開鍵暗号系を用いて転送元装置を特定し、公開鍵証明書を用いて第三者証明を実現し、フィンガープリントを用いて第三者情報を実現し、原本性情報の転送元装置が第1の装置であり、かつ、第2の装置が保持する第三者情報を示す第三者に、第三者証明の認証者が含まれることを検証することにより、第1の装置を検証し、信用できる第1の装置を特定する情報を直接に保持することなく、第1の装置が信用できるかどうかを判断することが可能となる。

## 【0044】

請求項7及び請求項24では、発行者装置が「信用する」第1の装置を示す利用者信任情報を用い、転送元の第1の装置が原本性情報の第1の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用できる第1の装置を発行者装置が指定することが可能となる。

請求項8及び請求項25では、発行者装置がデータの流通に関して「信用する」第1の装置を示す利用者信任情報を用い、転送元の第1の装置が原本性情報の第1の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用できる第1の装置を発行者装置がデータ毎、もしくは、データの集合毎に指定することが可能となる。

## 【0045】

請求項9及び請求項26では、原本性情報の第1の情報を自装置を示す情報として原本性を生成する手段と、生成した当該原本性情報を転送する手段を備えた発行者装置を提供することが可能となる。

請求項10及び請求項27では、発行者装置において、発行者装置の公開鍵のフィンガープリントを、原本性情報の第1の情報として用い、原本性情報を生成する。

## 【0046】

請求項 1 1 及び請求項 2 8 では、発行者装置において、MD 5 や SHA - 1 などの一方向関数によるデータのダイジェスト値を、原本性情報の第 2 の情報として用い、原本性情報を生成する。

請求項 1 2 及び請求項 2 9 では、発行者装置において、URL などのネットワーク上の識別子を、原本性情報の第 2 の情報として用い、原本性情報を生成する。

【 0 0 4 7 】

請求項 1 3 及び請求項 3 0 では、利用者装置において、原本性情報を転送する手段と、有効性を判別する手段とを備え、有効な原本性情報のみを格納する手段を備える。

請求項 1 4 及び請求項 3 1 では、利用者装置において、原本性情報を転送する際に、格納された原本性情報を消去する。

【 0 0 4 8 】

請求項 1 5 及び請求項 3 2 では、改札者装置において、有効性を判別する手段と、データを処理する手段を備え、有効な原本性情報の第 2 の情報が示すデータを処理する手段を備える。

請求項 1 6 及び請求項 3 3 では、改札者装置において、「正しい」発行者を示す発行者情報を備え、有効性を検証された原本性情報の第 1 の情報を示す発行者が発行者情報が示す発行者に含まれた場合に、原本性情報の第 2 の情報が示すデータを処理する。

【 0 0 4 9 】

請求項 1 7 及び請求項 3 4 では、上記で述べた発行者装置と、利用者装置と、改札者装置を有するシステムを構成することにより、これらの装置間において、チケット発行、チケットの譲渡、チケットの消費及びチケットの提示等の各処理を行うことが可能となる。

【 0 0 5 0 】

【発明の実施の形態】

最初に、権利を表象する電子情報である電子チケットをデータとして用いる場合における、原本データ流通システムにおけるデータ蓄積システムについて説明

する。

図 2 は、本発明の原本データ流通システムにおけるデータ蓄積システムの構成を示す。

【0051】

同図において、チケットの発行者は、発行者装置 1 を有し、チケットの発行先となる利用者は利用者装置 2 を有している。チケットの発行の際には、発行者装置 1 と利用者装置 2 の間は、接続装置 4 を介して通信手段が確立され、発行者装置 1 で有効化されたチケットを利用者装置 2 に転送する。

上記のこれらの装置は、図 2 (a), (b) などの構成をとることができる。

【0052】

同図 (a) は、利用者装置 2 として IC カードを用い、接続装置 4 として IC カードリーダライタを用いる際の代表的な構成を示し、同図 (b) は、利用者装置として IC カードなどの耐タンパ装置を装備可能もしくは、安全な場所に補間された PC を用い、接続装置 4 としてネットワークを用いる際の代表的な構成を示す。なお、同図 (a), (b) の構成を混在させて用いることも可能である。

【0053】

上記の通信手段は、チケットの発行の開始から終了までの間のみ確立させていればよい。以下、「譲渡」、「消費」、「提示」の際にもこれは同様である。

チケット譲渡の際には、発行時と同様に利用者装置 2 間で接続装置 4 を介して通信手段を確立し、有効なチケットを利用者装置 2 間で転送する。

チケットの改札者は、改札者装置 3 を有している。チケット消費の際には、発行時と同様に利用者装置 2 と改札者装置 3 との間で接続装置 4 を介して通信手段を確立し、利用者装置 2 から改札者装置 3 に有効なチケットを転送する。

【0054】

チケット提示の際には、2 つの利用者装置 2 の間、もしくは利用者装置 2 と改札者装置 3 との間で、接続装置 4 を介して通信手段を確立し、利用者装置 2 から他の利用者装置 2 もしくは、改札者装置 3 に有効なチケットを所持していることの証明を転送する。

このように、本発明に係るデータ蓄積システムは、一時的な相互通信手段を提

供する 1 つまたは、複数の接続装置 4 により接続された、1 つまたは、複数の発行者装置 1 と、1 つまたは、複数の利用者装置 2 と、1 つまたは、複数の改札者装置 3 とから構成されるシステムである。

【0055】

【実施例】

以下、図面と共に本発明の実施例を説明する。

図 3 から図 6 を用いて、上記のデータ蓄積システムを構成する各装置について説明する。

最初に、以下の説明で用いる式の意味を示す。

【0056】

$x \parallel y$  とは、 $x$  と  $y$  の接続である。

$H$  とは、一方向ハッシュ関数であり、 $y = H(x)$  を満たすような  $x$  を  $y$  から求めることが困難であるという性質を持つ。このようなハッシュ関数として、米 RSA 社の「MD 5」等が知られている。

$S_{pk}$  とは、検証関数  $V_{pk}$  により検証可能な電子署名  $S_{pk}(x)$  を生成する署名関数である。

【0057】

$V_{pk}$  は、検証関数であり、

$$V_{pk}(x, S_{pk}(x)) = 1, V_{pk}(x, other) = 0 \\ (other \neq S_{pk}(x))$$

という性質を持つ。即ち、電子署名  $S_{pk}(x)$  が  $x$  に対する  $S_{pk}$  による正しい署名であるかどうかを検証できる性質を持つ。

【0058】

$P_k$  は、検証鍵であり、検証器  $V$  に  $P_k$  を与えることにより、 $V_{pk}$  を構成することが可能であるという性質を持つ。検証鍵  $P_{k2}$  及び  $S_{pk1}$  による  $P_{k2}$  の電子署名  $S_{pk1}(P_{k2})$  の組  $(P_{k2}, S_{pk1}(P_{k2}))$  を特に、 $P_{k1}$  による  $P_{k2}$  の鍵証明書と呼ぶ。また、 $H(P_k)$  を特に、 $P_k$  のフィンガープリントと呼ぶ。

【0059】



以上で述べたような性質を持つ  $S_{pk}$ ,  $V_{pk}$  を実現するような電子署名方式として、日本電信電話の E S I G N などが知られている。

図 3 は、本発明の一実施例の発行者装置の構成を示す。

図 3 に示す発行者装置 1 は、制御部 11、署名部 12、データ生成部 13、トークン生成部 14、信頼情報生成部 15 から構成される。

#### 【0060】

制御部 11 は、検証鍵  $P_{kI}$  を保持し、チケットの流通を安全に行うための制御を行う。ここで、 $P_{kI}$  は、後述する署名部 12 が備える署名関数  $S_{pkI}$  に対応する検証鍵であり、そのフィンガープリント  $H(P_{kI})$  は、発行者を特定する識別子として用いられる。制御部 11 による制御の詳細については、後述する。

#### 【0061】

署名部 12 は、署名関数  $S_{pkI}$  を備える。 $S_{pkI}$  は、発行者装置 1 毎にそれぞれ異なり、署名部 12 により秘匿される。

データ生成部 13 は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データ  $m$  を生成する。本発明に係るデータ蓄積装置では、データ  $m$  の記述内容についてなんら制限を持つものではないため、データ  $m$  として切符やコンサートチケットなどの一般的チケットによって扱われる権利を表象する電子情報のほか、プログラム、音楽、画像データなどを扱うことが可能である。

#### 【0062】

トークン生成部 14 は、一方向ハッシュ関数  $H$  を備え、データ  $m$  及び検証鍵  $P_{kI}$  よりトークン

$$(c_1, c_2) = (H(m), H(P_{kI}))$$

を生成する。ここで、 $c_2$  は、トークン発行者情報であり、当該トークンの発行者を特定するフィンガープリントである。ここでは、 $c_1$  にデータ  $m$  のハッシュ値を用いたが、これには  $m$  を識別する識別子などを用いることも可能である。

#### 【0063】

信頼情報生成部 15 は、信頼情報  $(t_1, t_2, t_3)$  を生成する。 $(t_1,$

$t_2, t_3$ ) は、署名部 12 を用いて例えば、以下のように構成される。

$$t_1 = \{H(PkA_1), H(PkA_2), \dots, H(PkA_n)\}$$

$$t_2 = S_{PkI} (H(PkA_1) \parallel H(PkA_2) \parallel \dots \parallel H(PkA_n))$$

$$t_3 = PkI$$

ここで、 $H(PkA_i)$  は、発行者が「信用する」第三者（後述）を特定するフィンガープリントである。

【0064】

ここで、信任情報は以下で示す ( $t'_1, t'_2, t'_3, t'_4$ ) のように構成することも可能である。

$$t'_1 = \{H(PkA_1), H(PkA_2), \dots, H(PkA_n)\}$$

$$t'_2 = H(m)$$

$$t'_3 = S_{PkI} (H(PkA_1) \parallel H(PkA_2) \parallel \dots \parallel H(PkA_n) \parallel H(m))$$

$$t'_4 = PkI$$

この場合、 $H(PkA_i)$  は、発行者が「データ  $m$  を流通させるにあたって信用するに足りる」第三者を特定するフィンガープリントである。

【0065】

また、上記信任情報は、第三者がさらに信任情報を発行することにより再帰的に構築することも可能である。

また、さらに、信任情報を各発行者が生成することをせず、後述する利用者装置の耐タンパ装置の制御部や、改札者装置の制御部が予め固定的に保持しておく形態を採ることも可能である。この場合、署名は必要なく、以下で示す ( $t''_1, t''_2$ ) もしくは、 $t''_1$  のみとして信任情報を構成できる。

【0066】

$$t''_1 = \{H(PkA_1), H(PkA_2), \dots, H(PkA_n)\}$$

$$t''_2 = H(m)$$

この場合、 $H(PkA_i)$  は、当該制御部（を作成した第三者）が、「（データ  $m$  を流通させるにあたって）信用する」第三者を特定するフィンガープリントである。

【0067】

以下においては、信頼情報は  $(t_1, t_2, t_3)$  と構成されるものとして説明するが、上記のいずれの信頼情報を用いる場合も容易に類推可能である。

図4は、本発明の一実施例の利用者装置の構成を示す。

同図に示す利用者装置2は、制御部21、格納部22と、制御部23、認証部24、署名部25、番号生成部26、格納部27から構成される耐タンパ装置28を有する。耐タンパ装置28は、各構成部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンパ装置28として、ICカードや、ネットワーク経由で接続され、第三者により厳重に管理されたサーバなどが利用可能である。

【0068】

制御部21は、発行者情報

$$I_U = \{H(PkI_1), H(PkI_2), \dots, H(PkI_n), \}$$

を備え、耐タンパ装置28に封入された制御部23と共に、チケットの流通を安全に行うための制御を行う。ここで、 $I_U$  は、利用者から「信用された」発行者を示す集合であり、当該利用者により任意の時点で更新可能である。制御部21は、 $I_U$  に含まれる発行者により発行されたトークンのみを有効であると判断する。制御部21による制御の詳細については、後述する。

【0069】

格納部22は、利用者が保持するデータの集合 $M_U$  及び信頼情報の集合 $T_U$  を格納する。これらの集合は、制御部21により更新可能である。

制御部23は、検証鍵 $PkU$ 、 $PkA$ 及び鍵証明書 $(PkU, S_{PkA}(PkU))$ を保持し、制御部21と共に、チケットの流通を安全に行うための制御を行う。ここで、 $PkU$ は、署名部25が備える $S_{PkU}$  に対応する検証鍵であり、そのフィンガープリント $H(PkU)$  は、該利用者装置を特定する識別子として用いる。 $S_{PkA}$  は、ICカード製造者もしくは耐タンパサーバ管理者など、耐タンパ装置28の安全性を保証する第三者により秘匿される署名関数である。すなわち $S_{PkU}$  を含む耐タンパ装置28は、 $S_{PkA}$  を保持する第三者により耐タンパ性を保証されている。制御部23による制御の詳細については後述する。また、 $P$

$k_A$  は、 $S_{pkU}$  の検証鍵である。

【0070】

認証部 24 は、検証器 V を備える。

署名部 25 は、署名関数  $S_{pkU}$  を備える。 $S_{pkU}$  は、利用者装置 2 毎にそれぞれ異なり、署名部 25 により秘匿される。

番号生成部 26 は、次番号  $r_U$  を保持し、番号の払出しを要求されると当該時点の  $r_U$  の値を返却すると共に  $r_U$  をインクリメントする。ここで、 $r_U$  は正数である。

【0071】

格納部 27 は、トークンの集合  $C_U$  及び番号の集合  $R_U$  を格納する。これらの集合は、制御部 23 により更新可能である。

図 5 は、本発明の一実施例の改札者装置の構成を示す。

制御部 31 は、検証鍵  $P_{kE}$  及び、発行者情報

$$I_E = \{H(P_{kI_1}), H(P_{kI_2}), \dots, H(P_{kI_n}), \}$$

を備え、チケットの流通を安全に行うための制御を行う。ここで、 $I_E$  は、改札者から「信用された」発行者を示す集合であり、当該改札者により任意の時点で更新可能である。制御部 31 は、 $I_E$  に含まれる発行者により発行されたトークンのみを正当と判断し、当該トークンを伴うチケットの消費に対してのみサービスを提供する。制御部 31 による制御の詳細については後述する。

【0072】

認証部 32 は、検証器 V を備える。

番号生成部 33 は、次番号  $r_E$  を保持し、番号の払出しを要求されると該時点の  $r_E$  を返却すると共に、 $r_E$  をインクリメントする。ここで、 $r_E$  は正数である。

格納部 34 は、番号の集合  $R_E$  を格納する。これらの集合は、制御部 31 により更新可能である。

【0073】

図 6 は、本発明の一実施例の接続装置の構成を示す。

同図によれば、接続装置 4 は、通信部 41 から構成される。

通信部 41 は、発行者装置 1、利用者装置 2、改札者装置 3 間や、利用者装置 2 相互間での、一時的もしくは永続的な通信手段を提供する。ここで、接続装置 4 として、IC カード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数の PC（パーソナルコンピュータ）などが利用可能である。

## 【0074】

上述したような構成を有する各装置 1～4 を用いて電子チケットの流通を安全に行う方式を以下（1）チケットの発行の場合、（2）チケットの譲渡の場合、（3）チケットの検証の場合、のそれぞれの場合に分けて説明する。なお、各装置を跨がるそれぞれの通信は、接続装置 4 中の通信部 41 を介するものとする。

## （1） チケット発行の場合：

図 7 は、本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャートである。なお、同図では、発行者装置 1 と利用者装置 2 との間に存在する接続装置 4 は省略してある。

## 【0075】

ステップ 101) 発行者装置 1 の制御部 11 は、データ生成部 13 により、データ  $m$  を生成する。当該データ  $m$  を権利情報が記述されたチケットであるとする。

ステップ 102) 発行者装置 1 の制御部 11 は、トークン生成部 14 に  $m$  および  $PkI$  を与え、トークン  $(c_1, c_2) = (H(m), H(PkI))$  を生成する。

## 【0076】

ステップ 103) 制御部 11 は、信頼情報生成部 15 により、信頼情報  $(t_1, t_2, t_3)$  を生成する。信頼情報の構成は前述の通りである。

ステップ 104) 制御部 11 は、利用者装置 2 の制御部 21 に  $m$  と  $(t_1, t_2, t_3)$  を転送する。

ステップ 105) 利用者装置 2 の制御部 21 は、 $m$  を格納部 22 の  $M_U$  に、 $(t_1, t_2, t_3)$  を格納部 22 の  $T_U$  に、それぞれ追加して格納する。

## 【0077】

ステップ 106) 制御部 21 は、耐タンパ装置 28 の制御部 23 にセッション

ン情報 ( $s_1, s_2$ ) の生成を依頼し、制御部 23 は、以下の手順により ( $s_1, s_2$ ) を生成し、制御部 21 に転送する。

(a) 耐タンパ装置 28 の番号生成部 26 により番号  $r_U$  の払出しを受ける

【0078】

(b)  $r_U$  を格納部 27 の番号集合  $R_U$  に追加する。

(c) ( $s_1, s_2$ ) = ( $H(Pk_U), r_U$ ) を生成する。ここで、 $Pk_U$  は、制御部 21 が保持する検証鍵である。

ステップ 107) 制御部 21 は、発行者装置 1 の制御部 11 に ( $s_1, s_2$ ) を転送する。

【0079】

ステップ 108) 発行者装置 1 の制御部 11 は、署名部 12 が備える  $S_{Pk_I}$  と制御部 11 が保持する検証鍵  $Pk_I$  を用い、トークン交換形式  $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$  を得る。ここで、 $e$  の各要素は、以下の値となる。また、チケット発行の際においては  $e_7$  及び  $e_8$  はダミーであり、それぞれ任意の値を持たせてよい。

【0080】

$$e_1 = c_1$$

$$e_2 = c_2$$

$$e_3 = s_1$$

$$e_4 = s_2$$

$$e_5 = S_{Pk_I} (c_1 \parallel c_2 \parallel s_1 \parallel s_2)$$

$$e_6 = Pk_I$$

$$e_7 = any \text{ (任意)}$$

$$e_8 = any \text{ (任意)}$$

ステップ 109) 発行者装置 1 の制御部 11 は、利用者装置 2 の制御部 21 に  $e$  を転送する。

【0081】

ステップ 110) 利用者装置 2 の制御部 21 は、耐タンパ装置 28 の制御部

2 3 に  $e$  を転送し、 $e$  内のトークンの格納を依頼する。

ステップ 1 1 1) 耐タンパ装置 2 8 の制御部 2 3 は、認証部 2 4 を用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部 2 1 を介して、発行者装置 1 の制御部 1 1 に処理を中断を通知する。

【0 0 8 2】

$$e_3 = H(PkU) \quad (1)$$

$$e_4 \in R_U \quad (2)$$

$$V_{e6}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1 \quad (3)$$

$$e_2 = H(e_6) \quad (4)$$

上記の式 (1) 及び式 (2) は、セッション情報の正当性の検証である。この検証により、当該利用者装置 2 以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【0 0 8 3】

式 (3) は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

また、式 (4) は、トークン発行者情報の正当性の検証であり、当該トークンの署名者以外が発行者となるトークンを格納することを防止する。

ステップ 1 1 2) 利用者装置 2 の耐タンパ装置 2 8 の制御部 2 3 は、格納部 2 7 の  $R_U$  から  $e_4$  ( $= r_U$ ) を削除する。

【0 0 8 4】

ステップ 1 1 3) 耐タンパ装置 2 8 の制御部 2 3 は、格納部 2 7 の  $C_U$  に ( $e_1, e_2$ ) を追加する。

ステップ 1 1 4) 耐タンパ装置 2 8 の制御部 2 4 は、制御部 2 1 に ( $e_1, e_2$ ) を転送し、処理の正常終了を通知する。

ステップ 1 1 5) 制御部 2 1 は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は処理の正常終了を、発行者装置 1 の制御部 1 1 に通知する。

【0085】

$$e_1 = H(m) \quad (5)$$

$$e_2 \in I_U \quad (6)$$

式(5)及び式(6)は、転送されたトークンが、対象とするチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、発行されたチケットが有効であることを確認する。

【0086】

(2) チケット譲渡の場合：

以下は、利用者装置2aから利用者装置2bに対する、接続装置4を介したチケット譲渡処理の流れである。

図8、図9は、本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャートである。なお、同図において2つの利用者装置2a、2bの間に存在する接続装置4は省略してある。また、利用者装置2aの各構成要素の各々にはaを付し、利用者装置2bの各構成要素の各々にはbを付す。

【0087】

ステップ201) 利用者装置2aの制御部21aは、格納部22aが保持する $M_{Ua}$ から譲渡対象となるチケットmを抽出する。

ステップ202) 利用者装置2aの制御部21aは、格納部22aが保持する $T_{Ua}$ からmの発行者による信任情報( $t_1$ ,  $t_2$ ,  $t_3$ )を抽出する。

ステップ203) 制御部21aは、利用者装置2bの制御部21bにmと( $t_1$ ,  $t_2$ ,  $t_3$ )を転送する。

【0088】

ステップ204) 利用者装置2bの制御部21bは、mを格納部22bの $M_{Ub}$ に、( $t_1$ ,  $t_2$ ,  $t_3$ )を格納部22bの $T_{Ub}$ にそれぞれ格納する。

ステップ205) 制御部21bは、耐タンパ装置28bの制御部23bにセッション情報( $s_1$ ,  $s_2$ )の生成を依頼する。制御部23bは、以下の手順により( $s_1$ ,  $s_2$ )を生成し、制御部21bに転送する。

【0089】

(a) 耐タンパ装置28bの番号生成部26bにより番号 $r_{Ub}$ の払出しを受



ける。

(b)  $r_{Ub}$  を耐タンパ装置 28b の格納部 27b の番号集合  $R_{Ub}$  に追加する。

(c)  $(s_1, s_2) = (H(PkUb), r_{Ub})$  を生成する。ここで、 $PkUb$  は、制御部 21b が保持する検証鍵である。

【0090】

ステップ 206) 制御部 21b は、利用者装置 2 の制御部 21a に  $(s_1, s_2)$  を転送する。

ステップ 207) 利用者装置 2a の制御部 21a は、耐タンパ装置 28a の制御部 23a に  $(s_1, s_2)$  と譲渡対象チケットのハッシュ  $H(m)$  を転送する。

【0091】

ステップ 208) 利用者装置 2a の耐タンパ装置 28a の制御部 23a は、格納部 27a に格納された  $C_{Ua}$  について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部 21a に処理の失敗を通知する。

$$\exists c_1 \quad ((H(m), c_2) \in C_{Ua}) \quad (7)$$

式 (7) は、譲渡対象チケット  $m$  に対応するトークン  $(H(m), c_2)$  が耐タンパ装置 28 の格納部 27a に格納されていることも検証である。

【0092】

ステップ 209) 耐タンパ装置 28a の制御部 23a は、署名部 25a が備える  $S_{PkUa}$  と発行者装置 1 の制御部 11 が保持する検証鍵  $PkUa$ ,  $PkAa$  及び、鍵証明書  $(PkUa, S_{PkAa}(PkUa))$  を用い、トークン交換形式  $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$  を得る。ここで、 $e$  の各要素は以下の値をとる。

【0093】

$$e_1 = H(m)$$

$$e_2 = c_2$$

$$e_3 = s_1$$

$$e_4 = s_2$$

$$e_5 = S_{PkUa} (H(m) \parallel c_1 \parallel s_1 \parallel s_2)$$

$$e_6 = PkUa$$

$$e_7 = S_{PkAa} (PkUa)$$

$$e_8 = PkAa$$

ステップ210) 利用者装置2aの耐タンパ装置28aの制御装置23aは、 $s_2$ が正であるなら、 $C_{Ua}$ から $(H(m), c_2)$ を削除する。

【0094】

ステップ211) 耐タンパ装置28aの制御部23aは、制御部21aにeを転送する。

ステップ212) 制御部21aは、利用者装置2bの制御部21bにeを転送する。

ステップ213) 制御部21bは、耐タンパ装置28bの制御部23bにe、 $(t_1, t_2, t_3)$ を転送し、e内のトークンの格納を依頼する。

【0095】

ステップ214) 制御部23bは、認証部24bを用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部21bに処理の中断を通知する。

$$e_3 = H(PkUb) \quad (8)$$

$$e_4 \in R_{Ub} \quad (9)$$

$$V_{e6}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1 \quad (10)$$

$$V_{e6}(e_6, e_7) = 1 \quad (11)$$

$$H(e_8) \in t_1 \quad (12)$$

$$V_{t3}(t_1, t_2) = 1 \quad (13)$$

$$e_2 = H(t_3) \quad (14)$$

式(8)及び式(9)は、セッション情報の正当性の検証である。この検証により、当該利用者装置2b以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【0096】

式(10)は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

式(11)は、当該署名者の鍵証明書を検証である。また、式(12)は、該鍵証明書の署名者が、信頼情報中の信頼対象に含まれることの検証であり、式(13)は、該信頼情報の正当性の検証であり、式(14)は、該信頼情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンパ性が保証されていることを確認する。

【0097】

ステップ215) 利用者装置2の耐タンパ装置28bの制御部23bは、格納部27bの $R_{Ub}$ から $e_4 (= r_{Ub})$ を削除する。

ステップ216) 制御部23bは、格納部27bの $C_{Ub}$ に $(e_1, e_2)$ を追加する。

ステップ217) 制御部23bは、制御部21bに処理の正常終了を通知する。

【0098】

ステップ218) 制御部21bは、以下の式が成立することを検証する。検証に失敗した場合は処理の中断を、検証に成功した場合は処理の正常終了を、制御部21aに通知する。

$$e_1 = H(m) \quad (15)$$

$$e_2 \in I_{Ub} \quad (16)$$

式(15)及び式(16)は、転送されたトークンが、対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、譲渡されたチケットが有効であることを確認する。

【0099】

(3) チケット消費の場合：

以下は、利用者装置2から改札者装置3に対する接続装置4を介したチケット消費処理の流れである。

図 1 0 は、本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャートである。

【0 1 0 0】

なお、同図において、利用者装置 2 と改札者装置 3 間に存在する接続装置 4 は省略する。

ステップ 3 0 1) 利用者装置 2 の制御部 2 1 は、格納部 2 2 が保持する  $M_U$  から譲渡対象となるチケット  $m$  を抽出する。

ステップ 3 0 2) 制御部 2 1 は、格納部 2 2 が保持する  $T_U$  から  $m$  の発行者による信任情報  $(t_1, t_2, t_3)$  を抽出する。

【0 1 0 1】

ステップ 3 0 3) 制御部 2 1 は、改札者装置 3 の制御部 3 1 に  $m$  と  $(t_1, t_2, t_3)$  を転送する。

ステップ 3 0 4) 制御部 3 1 は、以下の手順により  $(s_1, s_2)$  を生成する。

(a) 番号生成部 3 3 により番号  $r_E$  の払出しを受ける。

【0 1 0 2】

(b)  $r_E$  を格納部 3 4 の番号集合  $R_E$  に追加する。

(c)  $(s_1, s_2) = (H(Pk_E), r_E)$  を生成する。ここで、 $Pk_E$  は制御部 3 1 が保持する検証鍵である。

ステップ 3 0 5) 制御部 3 1 は、利用者装置 2 の制御部 2 1 に  $(s_1, s_2)$  を転送する。

【0 1 0 3】

ステップ 3 0 6) 制御部 2 1 は、耐タンパ装置 2 8 の制御部 2 3 に  $(s_1, s_2)$  と消費対象チケットのハッシュ  $H(m)$  を転送する。

ステップ 3 0 7) 耐タンパ装置 2 8 の制御部 2 3 は、格納部 2 7 に格納された  $C_U$  について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部 2 1 に処理の失敗を通知する。

【0 1 0 4】

$$\exists c_2 ((H(m), c_2) \in C_U) \quad (17)$$

式(17)は、譲渡対象チケット $m$ に対応するトークン( $H(m)$ ,  $c_2$ )が耐タンパ装置28の格納部27に格納されていることの検証である。

ステップ308) 耐タンパ装置28の制御部23は、署名部25が備える $S_{PkU}$ と利用者装置2の制御部21が保持する検証鍵 $PkU$ ,  $PkA$ 及び、鍵証明書( $PkU$ ,  $S_{PkA}(PkU)$ )を用い、トークン交換形式 $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$ を得る。ここで、 $e$ の各要素は以下の値を採る。

【0105】

$$e_1 = H(m)$$

$$e_2 = c_2$$

$$e_3 = s_1$$

$$e_4 = s_2$$

$$e_5 = S_{PkU}(H(m) \parallel c_2 \parallel s_1 \parallel s_2)$$

$$e_6 = PkU$$

$$e_7 = S_{PkA}(PkU)$$

$$e_8 = PkA$$

ステップ309) 耐タンパ装置28の制御部23は、 $s_2$ が正であるなら、 $C_U$ から( $H(m)$ ,  $c_2$ )を削除する。

【0106】

ステップ310) 耐タンパ装置28の制御部23は、制御部21に $e$ を転送する。

ステップ311) 制御部21は、改札者装置3の制御部31に $e$ を転送する。

ステップ312) 認証部32を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、利用者装置2の制御部21の処理の中断を通知する。

【0107】

$$e_3 = H(PkE) \quad (18)$$

$$e_4 \in R_E \quad (19)$$

$$V_{e6}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1 \quad (20)$$

$$V_{e6}(e_6, e_7) = 1 \quad (21)$$

$$H(e_8) \in t_1 \quad (22)$$

$$V_{t3}(t_1, t_2) = 1 \quad (23)$$

$$e_2 = H(t_3) \quad (24)$$

式(18)及び式(19)は、セッション情報の正当性の検証である。この検証により、当該改札者装置3以外に宛られたトークン交換形式の利用や、トークン交換形式の再利用などによる不正を防止する。

#### 【0108】

式(20)は、トークン交換形式に対する署名の正当性の検証であり、この検証により、トークン交換形式の改竄を防止する。

式(21)は、当該署名者の鍵証明書を検証である。また、式(22)は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式(23)は、該信任情報の正当性の検証であり、式(24)は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンパ性が保証されていることを確認する。

#### 【0109】

ステップ313) 改札者装置3の制御部31は、格納部34の $R_E$ から $e_4$ (= $r_E$ )を削除する。

ステップ314) 制御部31は、以下の式が成立することを検証する。検証に失敗した場合は、処理に中断を利用者装置2の制御部21に通知する。検証に成功した場合は、 $m$ に対応するサービスをチケットの消費者に提供する。

#### 【0110】

$$e_1 = H(m) \quad (25)$$

$$e_2 \in I_E \quad (26)$$

式(25)及び式(26)は、転送されたトークンが対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、消費されたチケットが有効であることを確認する。

## 【0 1 1 1】

(4) チケット提示の場合：

チケット提示は、(3) チケット消費の場合の処理において、以下の変更を加えることにより可能になる。

・ステップ 3 0 4 の (c) において、 $(s_1, s_2) = (H(PkE), -r_E)$  を生成する。

## 【0 1 1 2】

・ステップ 3 1 2 において、式 (1 9) を  $-e_4 \in R_E$  とする。

以上の変更により、 $s_2$  が負数となるため、ステップ 3 0 9 において、 $C_U$  からの削除は行われず。即ち、送信側の利用者装置 2 に有効なチケットを残したまま、当該利用者装置 2 が該提示時点で有効なチケットを保持していることを検証すること、即ち、チケットの検札が可能となる。

## 【0 1 1 3】

なお、以上のそれぞれの場合 (1) ~ (4) の説明において、転送されたトークン交換形式は、明示的に保存しなかった。しかしながら、該トークン交換形式の格納部 2 2 などに保存しておき、該トークン交換形式及び m の受信の際に共に受信したトークン交換形式の履歴を m の送信の際に共に送信することにより、耐タンパ装置 2 8 が破られるなどして不正行為 (二重使用) が発見された場合に、不正が行われた装置を特定することが可能となる。

## 【0 1 1 4】

また、上記の実施例は、図 3 ~ 図 6 に示す構成に基づいて説明したが、この例に限定されることなく、発行者装置、利用者装置、改札者装置、及び接続装置の各機能をプログラムとして構築し、発行者装置、利用者装置、改札者装置、及び接続装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、CD-ROM 等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

## 【0 1 1 5】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

## 【0 1 1 6】

## 【発明の効果】

上述のように、本発明によれば、発行者が信用する経路のみを介してトークンを移送し、利用者や改札者が当該発行者を特定することにより、データに対応するトークンについて、該トークン内のトークン発行者情報が示す発行者以外により、該トークンをトークン格納部に新規に格納することを防止すると共に、該トークンが転送の過程において複数のトークン格納部に複製されることを防止する。

## 【0 1 1 7】

また、トークンを原本情報とし、特定の発行者により発行されたトークンを伴うデータのみを原本とすることにより、当該発行者が原本数を制限することが可能となる。

また、ネットワーク上に存在する情報の識別子（URLなど）をデータとして用いることにより、該情報の複製不能かつ譲渡可能なアクセス権を実現することができる。

## 【0 1 1 8】

また、権利内容を記述したチケットないし、当該チケットの識別子を本発明におけるデータとして用い、有効なトークンを伴うチケットのみを有効なチケットとし、利用者や改札者がそれ以外を無効なチケットとして拒否することにより、チケット自体を耐タンバ装置に格納することなしに、チケットの不正な行使（二重使用や不当な複製など）を防止することが可能となる。

## 【0 1 1 9】

また、プログラムを本発明におけるデータとして用い、特定の発行者により発行されたトークンを該プログラムの実行ライセンスとし、プログラムの実行器は、該トークンを伴うプログラム以外の実行を拒否することにより、不当に複製された該プログラムの実行を防止することが可能となる。

また、音楽データや画像データを本発明におけるデータとして用い、特定の発行者により発行されたトークンを該データの鑑賞権として用い、データの表示器もしくは、再生器は該トークンを伴うデータ以外を表示や再生を拒否することに



より、不当に複製された該データの鑑賞を防止することができる。

【図面の簡単な説明】

【図 1】

本発明の原理構成図である。

【図 2】

本発明の原本流通システムにおけるデータ蓄積システムの構成図である。

【図 3】

本発明の一実施例の発行者装置の構成図である。

【図 4】

本発明の一実施例の利用者装置の構成図である。

【図 5】

本発明の一実施例の改札者装置の構成図である。

【図 6】

本発明の一実施例の接続装置の構成図である。

【図 7】

本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャートである。

【図 8】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その 1）である。

【図 9】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その 2）である。

【図 1 0】

本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャートである。

【符号の説明】

- 1 発行者装置
- 2 利用者装置

3 改札者装置

4 接続装置

1 1 制御部

1 2 署名部

1 3 データ生成部

1 4 トークン生成部

1 5 信任情報生成部

2 1 制御部

2 2 格納部

2 3 制御部

2 4 認証部

2 5 署名部

2 6 番号生成部

2 7 格納部

2 8 耐タンパ装置

3 1 制御部

3 2 認証部

3 3 番号生成部

3 4 格納部

4 1 通信部

1 0 0 発行者装置

1 1 0 第 1 の原本性情報生成手段

1 2 0 第 1 の原本性情報転送手段

2 0 0 利用者装置

2 1 0 第 2 の原本性情報転送手段

2 2 0 第 1 の特定手段

2 3 0 第 1 の認証手段

2 4 0 格納手段

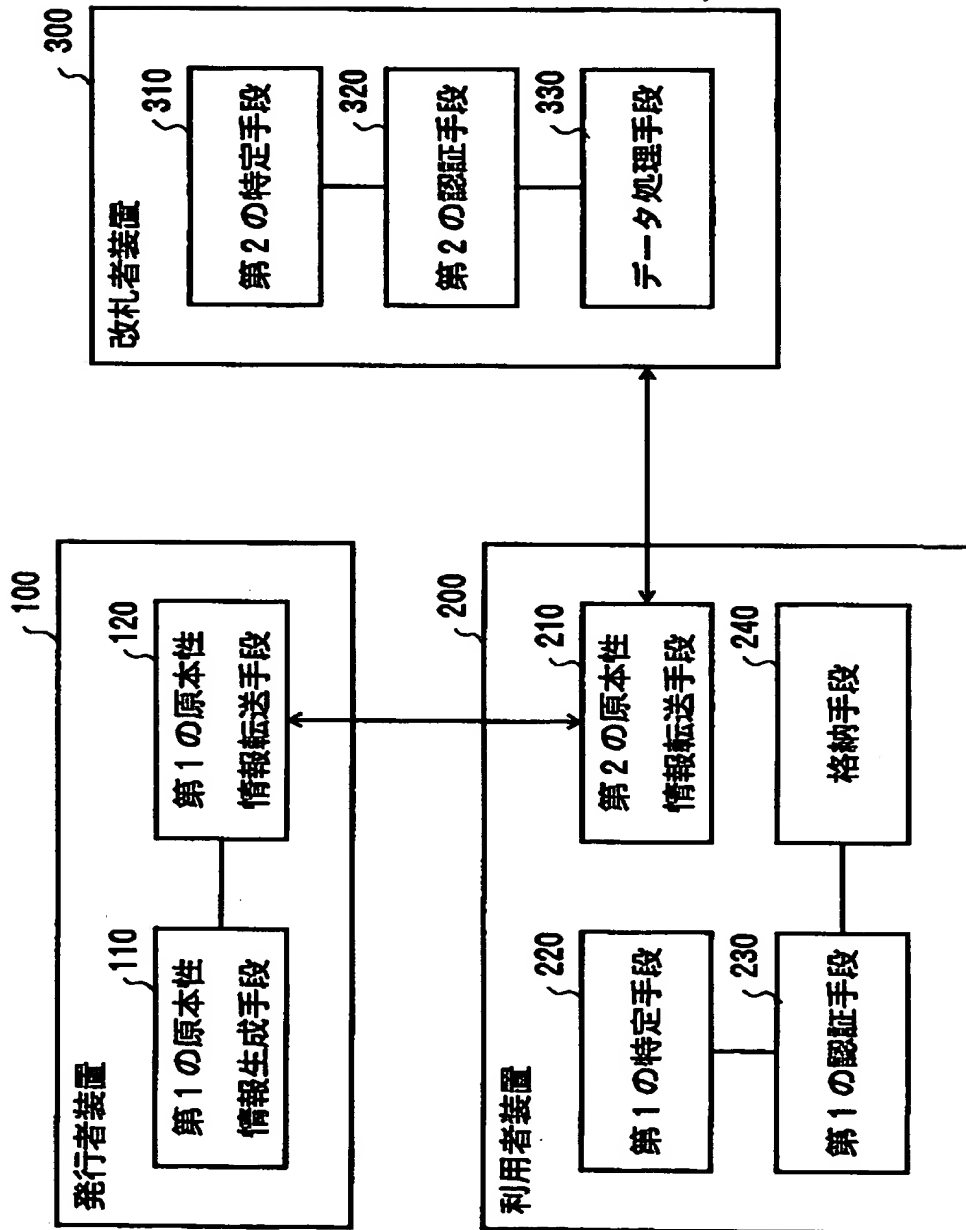
3 0 0 改札者装置

- 3 1 0 第 2 の特定手段
- 3 2 0 第 2 の認証手段
- 3 3 0 データ処理手段

【書類名】 図面

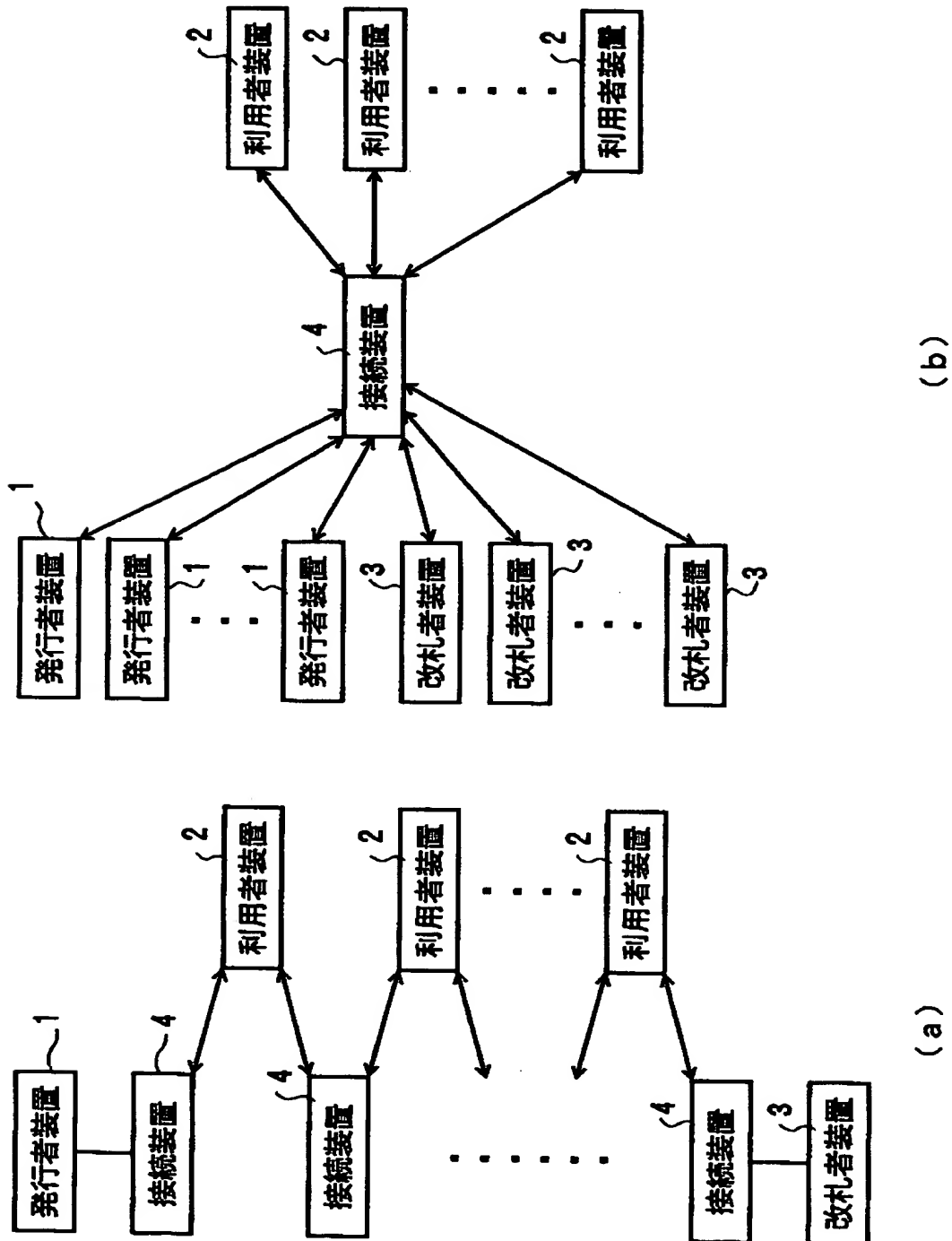
【図 1】

本発明の原理構成図



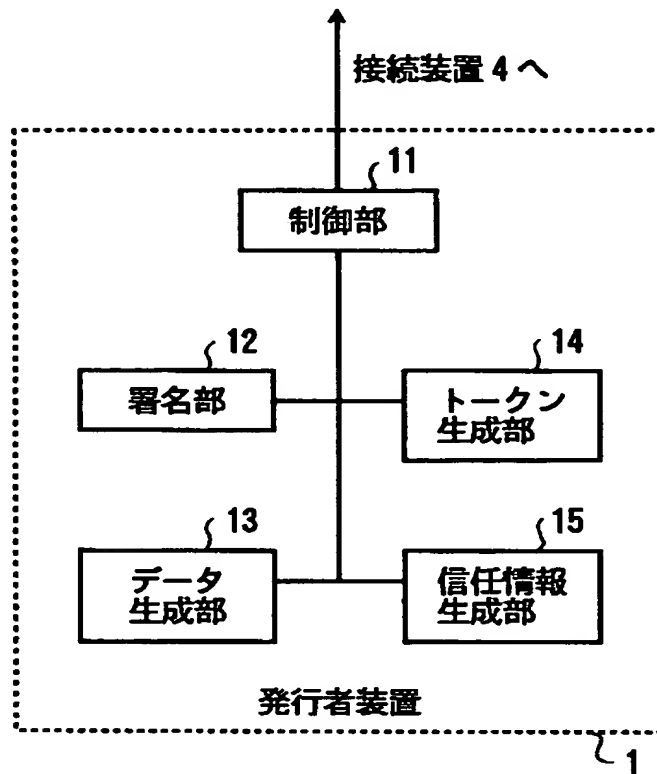
【図 2】

本発明の原本流通システムにおけるデータ蓄積システムの構成図



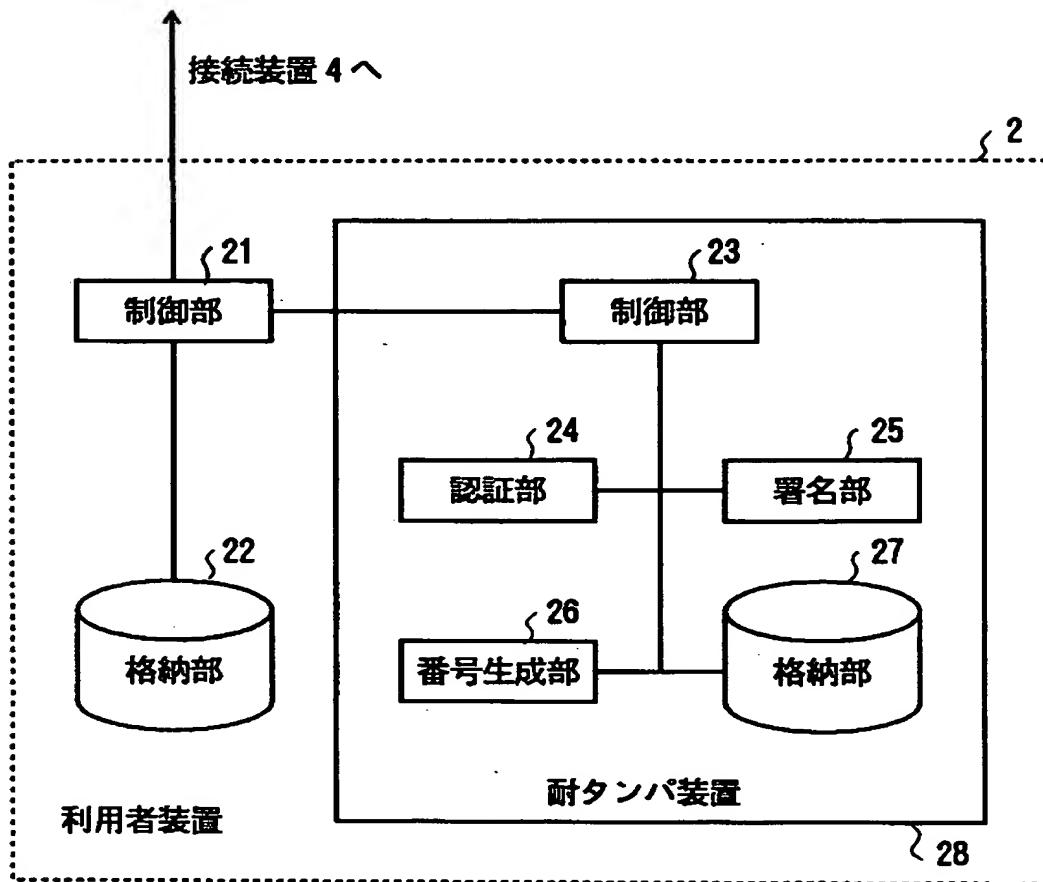
【図 3】

本発明の一実施例の発行者装置の構成図



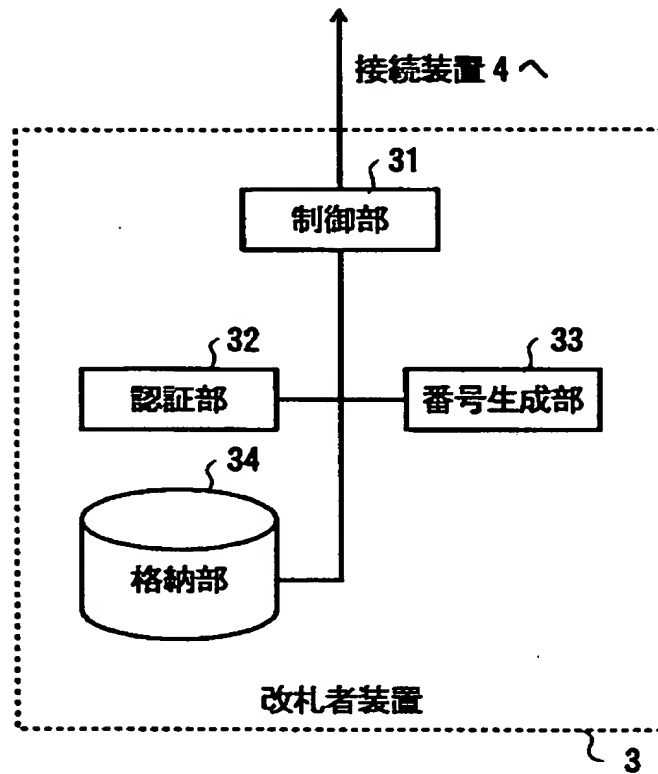
【図 4】

本発明の一実施例の利用者装置の構成図



【図 5】

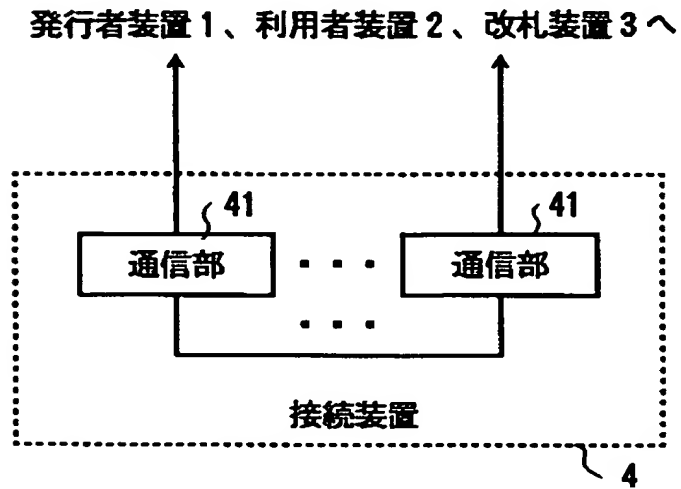
本発明の一実施例の改札者装置の構成図





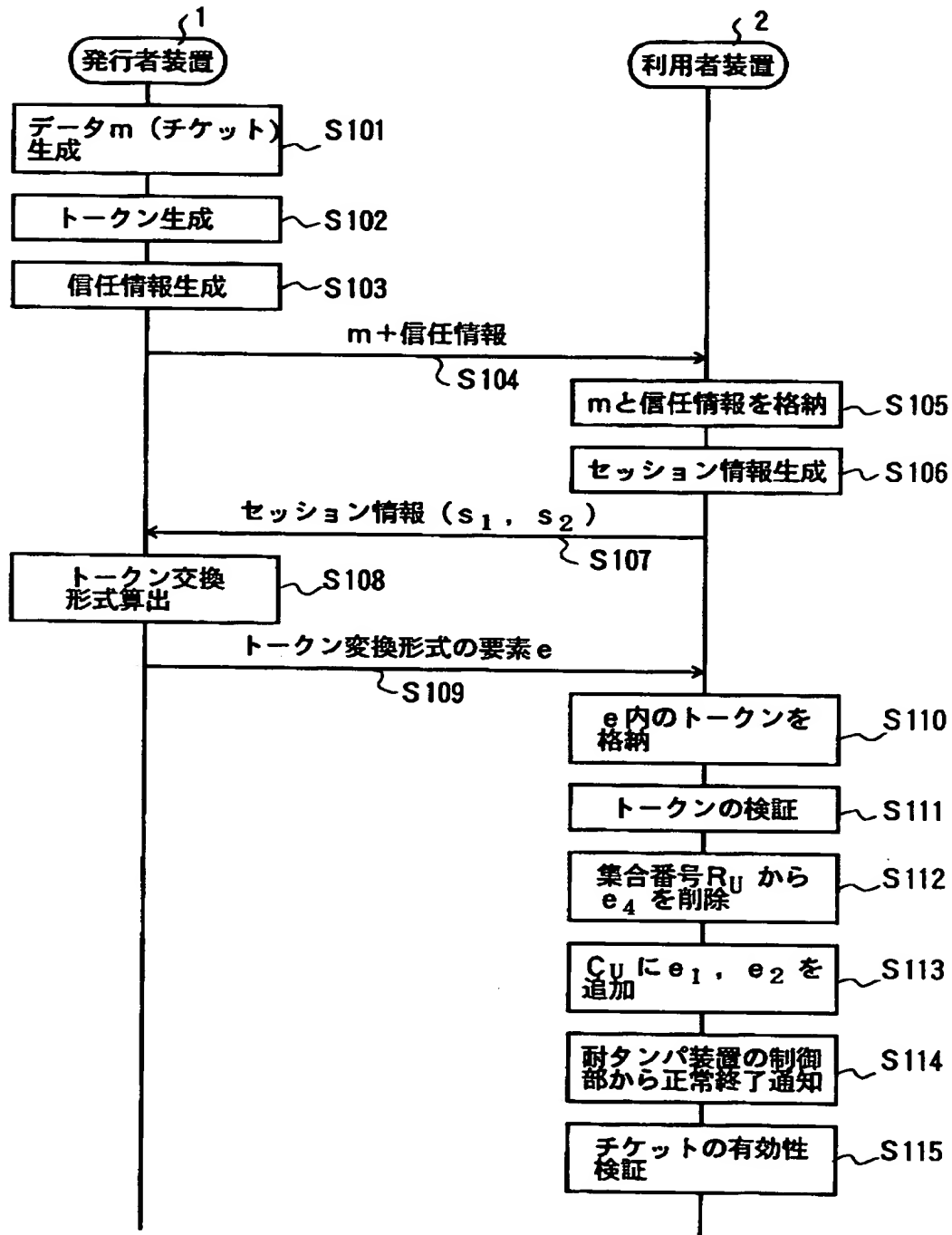
【図 6】

本発明の一実施例の接続装置の構成図



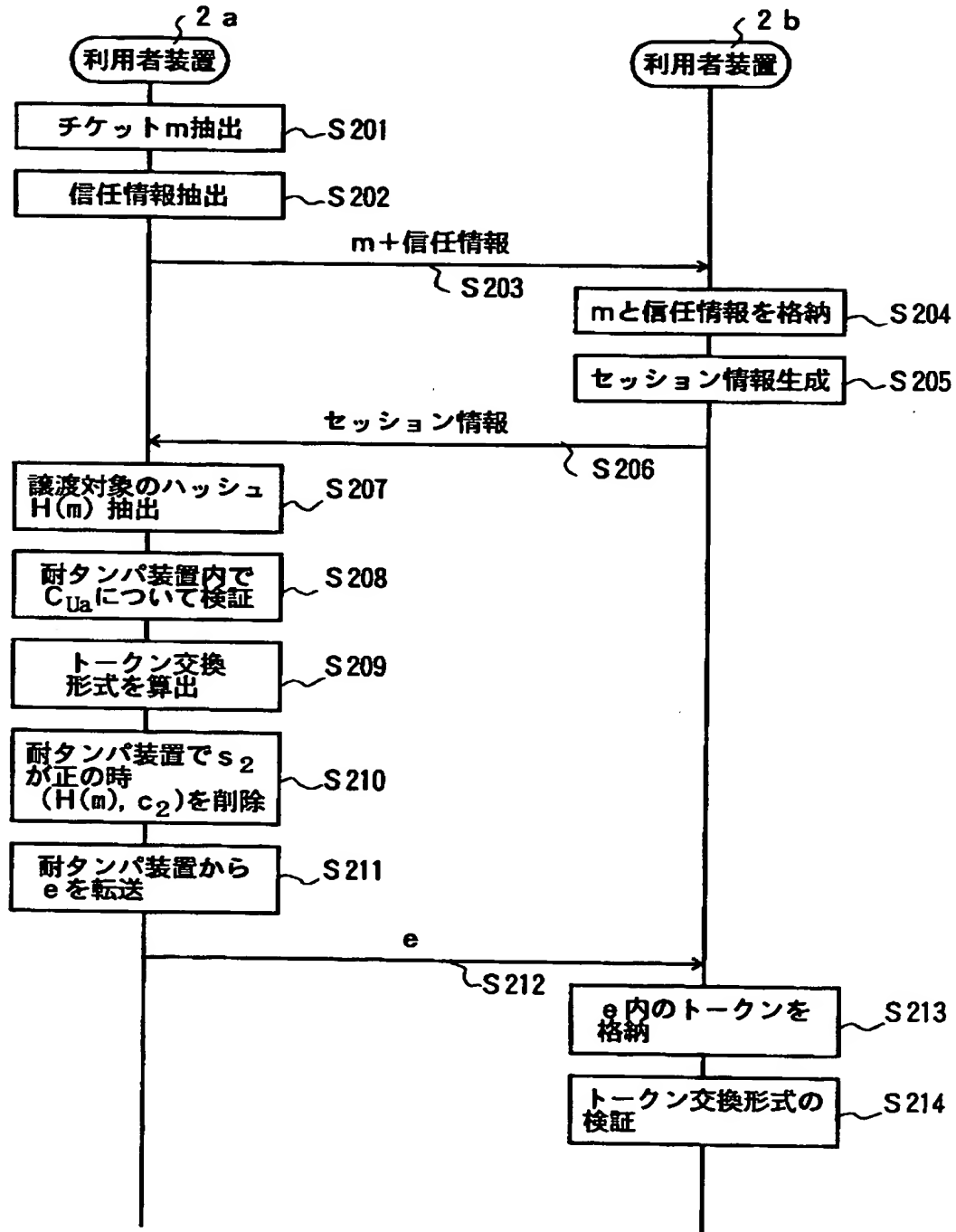
【図 7】

本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャート



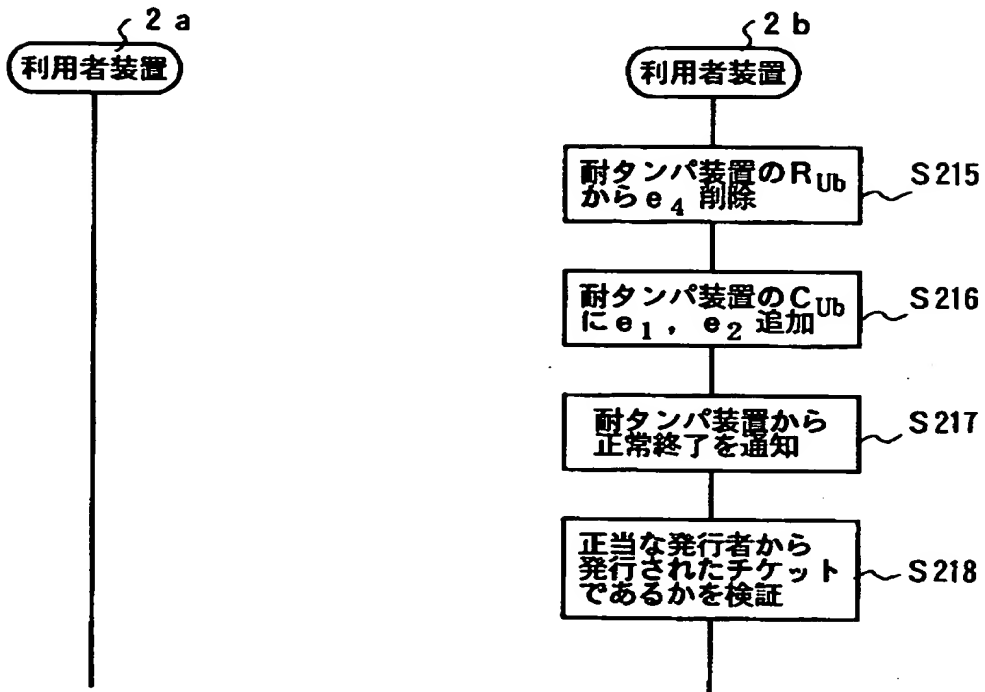
【図 8】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その 1）



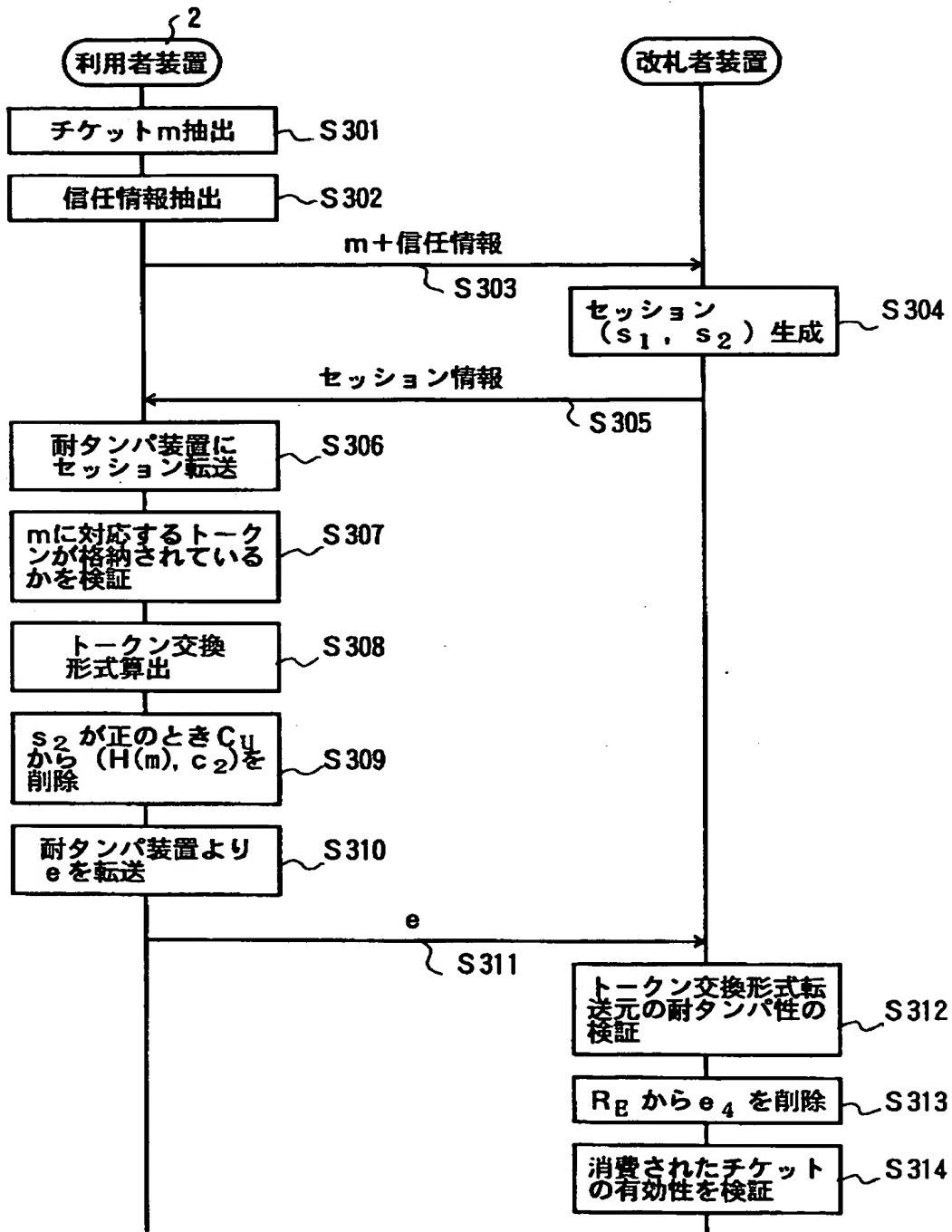
【図 9】

本発明の一実施例のチケット譲渡の場合の  
動作を示すシーケンスチャート（その 2）



【図 1 0】

本発明の一実施例のチケット消費の場合の  
動作を示すシーケンスチャート



【書類名】 要約書

【要約】

【課題】 トークンの生成やデータの流通などにおける負荷を低減する原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体を提供する。

【解決手段】 本発明は、ある装置に対応する第 1 の情報と、データもしくは、データに対応する情報である第 2 の情報と、から構成される原本性情報を転送する転送手段を有する第 1 の装置と、原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第 1 の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する認証手段とを有する第 2 の装置とを有する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社